

Amendments to the Claims:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) An apparatus for providing a trusted channel among secure operating systems (OSs) to which a mandatory access control (MAC) policy is applied, the apparatus comprising:

~~on a data~~ a data transmission side comprising:

a MAC module for providing MAC information of a user;

a kernel memory for specifying host addresses to which the trusted channel is to be applied and providing an encryption key for encryption of a packet and an authentication key for generation of authentication data; and

a trusted channel sub system for determining that determines, based upon MAC information from the MAC module and the host addresses to which a trusted channel is to be applied from the kernel memory, whether or not to apply the trusted channel, if data to user data to be transmitted to IP layer is provided from the user, by using the MAC information from the MAC module and the host addresses to which a trusted channel is to be applied from the kernel memory; creating a trusted channel header if the application of the trusted channel is determined; encrypting a specific portion of the packet; storing the authentication data in the trusted channel header; and transmitting the packet through a network; and

~~on a data~~ data reception side comprising:

a trusted channel sub system for investigating operable to determine whether the trusted channel is applied; retrieving to retrieve the authentication data in the trusted channel header; decrypting to decrypt the packet if the authentication data is valid; to conduct conducting trusted channel header processings; and transferring to transfer the packet to an upper level by following a routine for delivering the packet to an input processing section of the upper level to thereby provide the packet to a user on the data reception side; and

_____ a kernel memory for providing~~configured to provide~~ an authentication key ~~for the authentication of~~to authenticate the packet and an encryption key ~~for the decryption of~~to decrypt the packet;

_____ wherein the trusted channel header comprises authentication data operable to guarantee an integrity of the encrypted data, an initial vector for the decryption of the encrypted data, a next protocol field for a correct upper protocol processing, a header length for identifying a length of the header, a padding length for indicating a length of padding used for data encryption; and a MAC security class and a MAC category for delivering the MAC information of the user.

2. (Currently Amended) The apparatus of claim 1, wherein ~~the application of the trusted channel is determined in case of data transmission, if two~~ applied when both of following requirements are satisfied: a destination address of the packet ~~should~~ corresponds to one of the host addresses to which the trusted channel is applied and the user ~~should have~~has a MAC security class; and

_____ wherein if the application of the trusted channel is determined, the application of the trusted channel is indicated in a next protocol field of an IP header of the packet.

3. (Currently Amended) The apparatus of claim 2, wherein on the data reception side, the application of the trusted channel is ~~investigated, in case of data reception,~~determined by checking whether the next protocol field ~~of the IP header of the packet~~ represents the trusted channel header.

4. (Canceled).

5. (Currently Amended) The apparatus of ~~claim 1~~claim 1, wherein the packet, except for encryption area of the packet for maintaining security of the packet is set to be all areas thereof excluding an IP header area, the authentication data area, and the initial vector area is encrypted.

6. (Currently Amended) A method for providing a trusted channel among secure operating systems (OSs) including a trusted channel sub system and a kernel memory on each of a data transmission side and a data reception side and a MAC module on the data transmission side, the method comprising the steps of:

(a) applying a trusted channel to a user provided packet to be transmitted to the IP layer, based upon the executing execution of a packet output routine of an Internet Protocol (IP) layer if data to be transmitted to the IP layer is provided from the user; and that searching searches the MAC module and the kernel memory on the data transmission side ~~to determine whether or not to apply a trusted channel to a corresponding packet;~~

(b) creating a trusted channel header for storing therein information generated at a time when the trusted channel is applied and security information, i.e., a MAC security class and a MAC category, of the of the user if the application of the trusted channel is determined applied in the in step (a);

(c) encrypting all areas of the trusted channel header excluding an authentication data portion and an initial vector portion; generating authentication information for an integrity of validating the packet; and storing the authentication information in the trusted channel header;

(d) conducting a checksum processing and a fragmentation processing for of the IP packet packet and providing the packet to the trusted channel sub system on the data reception side through a network by following a lower level output routine;

(e) performing reassembling and checksum processing, at a reception side IP input processing unit, a reassembling processing and a checksum processing, at a reception side IP input processing unit, for the packet received at the trusted channel sub system on the data reception side through the network and investigating determining whether the trusted channel is applied to the packet by examining a next protocol field of an IP header in order to decrypt the packet;

(f) retrieving the authentication data in the trusted channel header before decrypting the packet if it is found in the step (e) that the trusted channel is applied to the packet and decrypting the packet if the authentication data is valid while discarding the packet if the authentication data is not valid; and

(g) transferring the decrypted packet to an upper level by following a routine for delivering the packet to an input processing section of an upper level to thereby provide the packet to a user on the data reception side;

wherein the trusted channel header includes a 128-bit authentication data field containing the authentication information for the encrypted packet, a 64-bit initial vector field used as encryption synchronization data of an encryption algorithm, a 8-bit next header field identifying an upper level protocol of IP, a 4-bit trusted channel header length field indicating a length in bytes of the trusted channel header, a 4-bit padding length field designating a length in bytes of a padding used for the encryption of the packet, and a 16-bit MAC security class field and a 64-bit MAC category field showing MAC information of the user who requests the communication.

7. (Currently Amended) The method of claim 6, wherein ~~the application of the~~ applying of the trusted channel is determined in the in step (a) is determined by examining whether a destination address of the packet corresponds to one of the host addresses to which the trusted channel is applied and whether the user has a MAC security class.

8. (Currently Amended) The method of claim 6, wherein the trusted channel header is recorded in the next protocol field of an IP header of the packet to inform the user on the data reception side ~~of the fact that~~ the trusted channel is applied to the packet.

9. (Canceled).